Privacy Impact Assessment
for

USALearning®

February 8, 2018

Point of Contact

Willie Harrison
Director, Learning Management Systems
USALearning®

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The Office of Personnel Management (OPM), USALearning® Program Office works in collaboration with contractors that are responsible for Learning Management Systems (LMS) used by Federal government employees. The purpose of these systems is to deliver online training for various federal agencies through an online interface. The applications are developed to comply with e-Learning standards while providing OPM with a comprehensive LMS and delivering a variety of training courseware content. This PIA is being conducted because the systems used by the Program Office collect, maintain, and use personally identifiable information.

Overview

USALearning® is the official learning and development office for the United States Federal Government and supports the development of the Federal workforce by supporting agency missions of quality e-Learning products, information, and services. The purpose of the program is to leverage simplified acquisition processes and allow agencies to expeditiously acquire an LMS and other course delivery platforms customized for one-time or continual use as client requirements dictate. An LMS allows employees to create, track, manage and distribute learning materials of any kind, on-site at an agency or virtually.

The contracted systems used by USALearning® are OPM owned, Commercial Off-the-Shelf products that are managed by contractors. They are web-based LMS using two major components – application/web servers and database servers.

USALearning® applications and contracted systems allow agencies to expeditiously acquire a myriad of support and training services and to leverage simplified acquisition processes via Intra/Interagency agreements under the authority of the Economy Act (31 U.S.C. § 1535) and Revolving Fund (5 U.S.C. § 1304(e)), while using and Federal Acquisition Regulation 17.5. For example, an agency can use OPM's contracts to create an LMS that will allow that agency's employees to access their personal training

plan, learning history, course catalogs, view training progress, request training electronically, and launch web-based training.

The LMSs also assist in federal reporting requirements. All government agencies are mandated to submit their training records to the Enterprise Human Resources Integration Data Warehouse (EHRIDW) on a monthly basis. The Data Warehouse is the main repository for the Federal employee workforce information. It holds all available historical human resource, payroll, and training data for title 5, Executive Branch employees and provides business intelligence applications for HR specialists in the Federal government, as well as online access to a Federal worker's employment records.

Section 1. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The legal authorities to gather and use the information are outlined 5 U.S.C. §§ 4115, 4117 and 4118 and Executive Order (EO) 11248. EO 11248 assigns additional responsibilities to OPM for planning and promoting the development, improvement, coordination, and evaluation of training in accordance with 5 U.S.C. Chapter 41 and policy set forth in the Executive Order. Additional authorities for sharing, leveraging and acquiring shared services are contained in the Economy Act, 31 U.S.C. § 1535 and Federal Acquisition Regulation 17.5 and the Revolving Fund, 5 U.S.C. § 1304(e).

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The Privacy Act SORN that applies to the information is OPM/GOVT-1 General Personnel Records, available at www.opm.gov/privacy.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

The system security plan has been completed as part of the Authority to Operate (ATO) that was granted in February 2016.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. The OPM Records Office is working with the program office to inventory the records appropriately, schedule the records and obtain approval through NARA. These records are currently being treated as permanent.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information is not covered by the Paperwork Reduction Act because the system only handles electronic collections for Federal government employees.

Section 2. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The systems may contain PII obtained by customer agencies. This includes employee information, such as full name, date of birth, job title, pay plan, Social Security number, and organization information, such as agency/organization name, address, description, and other associated information. The exact information collected, used, disseminated and maintained is determined by the customer agency.

All data extracts regarding employees and organizations are exported to customer agencies. The extract includes employee identifying information and course completion information. This information is returned to the requesting agency for the purpose of updating and maintaining employee training records.

2.2. What are the sources of the information and how is the information collected for the project?

The LMSs collect information directly from the customer agency through a web-based interface. Information collected by the customer agency comes directly from the Human Resources Office where personnel data is uploaded nightly.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. The system does not use any information from commercial sources and does not use any publicly available information.

2.4. Discuss how accuracy of the data is ensured.

The system does not verify the accuracy of the information it receives. Users are responsible for reviewing their own user profile to ensure the accuracy of the information. If individuals using the web interface find inaccuracies regarding their data they are directed to their agency's LMS administrator. The agency's LMS administrator is responsible for the accuracy of training records in the system.

2.5. <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

<u>Privacy Risk:</u> There is a risk that the information in the system is not accurate, or that the information is incomplete, resulting in a user account profile that does not reflect the training record of an individual.

<u>Mitigation:</u> This risk is not mitigated directly by the system. However, since all individuals are required to review their profile information before submitting it to OPM, it is assumed to be accurate when coming from the individual. Additionally, both the individuals and the agency LMS administrators have the ability to review and update any inaccurate information by contacting the related agency's LMS administrator.

Additionally, customer agency representatives verify the employee's information before it is uploaded into the system.

Privacy Risk: There is a risk that more information than is needed to meet the business purpose of the system is collected.

Mitigation: This risk is mitigated by requesting only the information that is needed for the training purposes, but is the responsibility of the customer agency. The OPM program office discusses with each customer agency representative what information is needed to preclude unnecessary information being collected. This process ensures the only required information is collected.

Section 3. Uses of the Information

3.1. Describe how and why the project uses the information.

The purpose of the USALearning® Program Office is to deliver training for various federal agencies via an online interface. The applications are developed to comply with e-Learning standards while providing customer agencies with a comprehensive LMS and delivering a variety of training courseware content. USALearning® specifically uses the information collected in the LMSs to provide online training courses and curricula to Federal agencies to satisfy the government required e-Training initiatives. The e-Training initiatives have been implemented and successfully adopted by most Federal agencies. E-Training is one of twenty-four e-Government initiatives outlined in the President's Management Agenda, for making the Federal government more focused on citizens and results, and one of five e-Government initiatives managed by OPM. The information collected on the LMSs is sent by the vendors to OPM's EHRI data warehouse on a monthly basis. All Federal government agencies are required to submit training records to the EHRI data warehouse monthly. The EHRI data warehouse is the main repository for Federal employee workforce information.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

The system uses internal tools only to search and query features and enable OPM and customer agencies to run reports. The system does not use any other tools, programs, or other technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3. Are there other programs/offices with assigned roles and responsibilities within the system?

USALearning® Program Office employees, contractors that manage the systems, and officials designated by the customer agencies have access to the system as assigned according to their roles and responsibilities. No other OPM offices have direct access to the system, although the EHRI data warehouse employees have access to the information sent monthly.

3.4. <u>Privacy Impact Analysis</u>: Related to the Uses of Information

<u>Privacy Risk</u>: There is a risk of unintentional disclosure of PII to unauthorized individuals or entities while data is in transit between the system and the customer agency or the EHRI data warehouse.

<u>Mitigation</u>: This risk is mitigated through the use of secure, encrypted connections, documented in Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU), as well as through providing users with security and privacy awareness training.

<u>Privacy Risk</u>: There is a risk that an unauthorized person may access the information in the system or that an authorized person may access the information in the system for an unauthorized purpose.

Mitigation: This risk is mitigated through the use of role-based access controls, unique user IDs and passwords for access, and audit systems.

Section 4. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Each customer agency provides a Privacy Act statement to its employees, which notifies the individual about the authority to collect the information requested, the purposes for which it will be used, other routine uses of the information, and the consequences of declining to provide the information. OPM provides guidance to the customer agency regarding the statement but does not review the content. The customer agency determines where and how the Privacy Act statement is displayed on their view of each LMS. In addition to the Privacy Act statements, this PIA and the SORN referenced in Section 1.4 also provide notice to the individual users..

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals are informed through Privacy Act statements that providing information is voluntary but that failure to provide the information will result in no access to the system. The individual does not have the opportunity to consent to specific uses of the information.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive notice concerning why their information is being collected and what it will be used for.

Mitigation: This risk is mitigated by the customer agency providing a Privacy Act statement to their individual users. The statement is typically displayed on the LMS homepage.

Section 5. Data Retention by the project

5.1. Explain how long and for what reason the information is retained.

For typical business needs, personal information and training data about an individual in this system should be retained for 5 years or when superseded or obsolete. However, there is currently no records schedule in place for these records and, therefore, they are currently being treated as permanent.

5.2. <u>Privacy Impact Analysis</u>: Related to Retention

Privacy Risk: There is a risk that the records in the system will be retained for longer than is necessary to meet the business need for which they were collected.

Mitigation: The Program Office is working to mitigate this risk by developing the appropriate records schedule. Until that records schedule is in place, this risk remains as the records must be considered permanent.

Section 6. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. Training data is shared with customer agencies. Only administrators of the LMSs have access to the data. Memorandums of Understanding and Interconnection Security Agreements between OPM and its customer agencies are used to establish an agreement on policies and procedures, and Points of Contact.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any external sharing from noted in 6.1 described above is compatible with SORN OPM/GOVT-1 General Personnel Records. The purpose for the collection of information is to gather records reflecting work experience and specialized education or training obtained by Federal employees.

USALearning® provides information to contractors who conduct the training curriculum on its behalf. The SORN contains the following routine uses that permit this sharing:

(a) To disclose information to Government training facilities (Federal, State, and local) and to non-Government training facilities (private vendors of training courses or programs, private schools, etc.) for training purposes.

(t). To provide an official of another Federal agency information needed in the performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected and maintained.

(jj). To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

6.3. Does the project place limitations on re-dissemination?

There are no specific limitations placed on re-dissemination of the information in the system. However, the customer agencies and contractors who have access to the information are governed by their respective ISAs, MOUs, and contracts, as well as by the system of records notice referenced in Section 1.4.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The system can create an audit report to track information returning to the customer agencies.

6.5. <u>Privacy Impact Analysis</u>: Related to Information Sharing

<u>Privacy Risk</u>: There is a risk that information in the system will be shared for a purpose other than that for which it was collected.

<u>Mitigation</u>: This risk is mitigated by entering into ISAs and MOUs with the customer agencies so that their users are informed regarding the purpose and use of the information. In addition, role-based access controls, unique

user IDs and passwords for access, are employed so that only those with a need to know have access to the information.

Section 7. Redress

7.1. What are the procedures that allow individuals to access their information?

Once inside the web-based application, individuals can navigate to review their record of completed courses. However, they do not have direct system access to other information that the LMS contains about them. Individuals who want to access the records contained in the system should contact the appropriate employing agency office, as outlined in the OPM/GOVT 1 General Personnel Records SORN.

Individuals must furnish the following information for their records to be located and identified: full name, date of birth, Social Security number, last employing agency and approximate dates of employment (for former Federal employees), and signature. In addition, individuals requesting access must also comply with the OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals cannot edit their information in the system. If incorrect information is found in the system, they may contact their agency's Human Resources Office or LMS administrator to correct the information. In addition, individuals may request an amendment to their information by following the procedure described in Section 7.1.

7.3. How does the project notify individuals about the

Individuals are notified via the employing agency on the procedures for correcting their information, through the applicable SORN, and through this PIA.

7.4. <u>Privacy Impact Analysis</u>: Related to Redress

<u>Privacy Risk:</u> There is a risk that individual users will not understand that they can access and correct their training records and correct any erroneous information.

<u>Mitigation:</u> This risk is mitigated by providing users with information about how to access and amend their records. If users find inaccurate training information, they can contact their agency-based LMS administrator(s). The administrator has the ability to research and remediate incorrect information. In addition, individuals may follow the procedures for amending records outlined in the OPM/GOVT 1 SORN.

Section 8. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in this PIA?

USALearning® ensures that the practices stated in this PIA are followed by leveraging training, policies, the OPM Information Technologies Rules of Behavior requirements, and auditing and accounting.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All Federal government personnel and contractors are required to take annual Security and Privacy Awareness training. It is the customer agencies' responsibility to ensure that their employees complete the required training.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Each customer agency has a designated agency-based LMS administrator who follows agency guidance to grant appropriate access to individuals at their respective agency.

Contractors that have access to the system are determined internally based on customer requirements, skill level, and resource availability.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The USALearning® program enters into Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU) with customer agencies. These MOUs and ISAs are used to establish policies and procedures related to the description and use of information and to designate points of contact at the customer agencies. MOUs and ISAs are valid for 3 years unless changes are required. These documents are routinely reviewed by USALearning® Program Office staff as part of annual assessments of the LMSs. If a change is required, both parties review and sign the updated documents.

Responsible Officials

Joseph Kennedy
Associate Director
Human Resources Solutions

Willie Harrison
Director, Learning Management Systems
USALearning®

Approval Signature

Signed Copy on File with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer